Examples
Cyclic codes

13^{th} February, 2006

1. Show whether the sets $\{(0,1,1,2),(2,0,1,1),(1,2,0,1),(1,1,2,0)\} \subset \mathbf{F}_3^4$ and $\{11111\} \subset \mathbf{F}_2^5$ are cyclic codes.

Solution. Both are cyclic sets since $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is in S for all $(a_0, \ldots, a_{n-1})$ in S. But for the former set $0112 + 2011 = 2120$, which is not in the set, therefore the set is not a cyclic code.

#

Similarly for the latter, since $11111 + 11111 = 00000$, not in the set. Hence this set is also not a cyclic code.

#

2. Show that in a the ring $\mathbf{F}_2[x]/\left(x^3-1\right)$ the subset $I = \left\{0, 1+x, x+x^2, 1+x^2\right\}$ is an ideal.

Solution.A non-empty subset I of a ring R is an ideal if both $a+b$ and $a-b$ belong to I for all a and b in I, and if $r \cdot a \in I$ for all r in R and a in I. Here $q = 2$, from which we know that $a + b = a - b$. Since

$$\left.\begin{array}{cc} 0+1+x & =1+x \\ 0+x+x^2 & =x+x^2 \\ 1+x+x+x^2 & =1+x^2 \\ 1+x+1+x^2 & =x+x^2 \\ x+x^2+x+x^2 & =0 \\ x+x^2+1+x^2 & =1+x \end{array}\right\} \in I$$

Next, the ring R being

$$\mathbf{F}_2[x]/\left(x^3-1\right) = \left\{0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2\right\}$$

and its subset to consider

$$I = \left\{0, 1+x, x+x^2, 1+x^2\right\}$$

the multiplication table of $r \cdot a$ for all $r \in R$ and $a \in I$ is

$\cdot$	0	$1+x$	$1+x^2$	$x+x^2$
0	0	0	0	0
1	0	$1+x$	$1+x^2$	$x+x^2$
x	0	$x+x^2$	$1+x$	$1+x^2$
$1+x$	0	$1+x^2$	$x+x^2$	$1+x$
x^2	0	$1+x^2$	$x+x^2$	$1+x$
$1+x^2$	0	$x+x^2$	$1+x$	$1+x^2$
$x+x^2$	0	$1+x$	$1+x^2$	$x+x^2$
$1+x+x^2$	0	0	0	0

Table 1. $r \cdot a$ for all $r \in R$ and $a \in I$

From Table 1 we can see that $r \cdot a$ is in I. Hence we conclude that the subset I of R is an ideal.

#

3. Find how many binary cyclic codes of length 6 there are. Give one cyclic code as an example.

Solution. First we factorise the polynomial $x^6 - 1 \in \mathbf{F}_2[x]$ thus,

$$x^6 - 1 = (1+x)^2 \left(1+x+x^2\right)^2$$

Next, list all the monic divisors of $x^6 - 1$,

$$1, \quad 1+x, \quad 1+x+x^2, \quad (1+x)^2, \quad (1+x)\left(1+x+x^2\right),$$

$$(1+x)^2\left(1+x+x^2\right),\quad \left(1+x+x^2\right)^2,\quad (1+x)\left(1+x+x^2\right)^2,\quad \left(1+x^6\right)$$

Since the nuber of these is nine, there are nine binary codes of length 6. We can then write down all these cyclic codes based on the map π, for example the one corresponding to the polynomial $\left(1+x+x^2\right)^2$ is found by

$$\left(1+x+x^2\right)^2=\left(1+x+x^2\right)\left(1+x+x^2\right)=1+x^2+x^4$$

$$\begin{array}{lll} 0\cdot\left(1+x^2+x^4\right) & =0 & \to \quad 000000\\ 1\cdot\left(1+x^2+x^4\right) & =1+x^2+x^4 & \to \quad 101010\\ x\cdot\left(1+x^2+x^4\right) & =x+x^3+x^5 & \to \quad 010101 \end{array}$$

Then all the additions among these give another word, $010101+101010=111111$. Hence the cyclic code is

$$\{000000,101010,010101,111111\}$$

#

4. Based on the factorisation $x^7-1=(1+x)\left(1+x^2+x^3\right)\left(1+x+x^3\right)\in\mathbf{F}_2[x]$. Find the number of different binary $[7,3]$-cyclic codes,

Solution. First we list all the 8 monic divisors of x^7-1,

$$1,\quad 1+x,\quad \left(1+x^2+x^3\right),\quad \left(1+x+x^3\right),\quad (1+x)\left(1+x^2+x^3\right),\quad (1+x)\left(1+x+x^3\right),$$
$$\left(1+x^2+x^3\right)\left(1+x+x^3\right),\quad (1+x)\left(1+x^2+x^3\right)\left(1+x+x^3\right)$$

We need a code for which the dimention is $k=3$. Write all the bases of each of these monic divisors.

$$\begin{array}{lll} 1,x,x^2,\ldots,x^6 & \to & \text{k=7}\\ 1+x,x+x^2,x^2+x^3,\ldots,x^5+x^6 & \to & k=6\\ \left(1+x^2+x^3\right) & \to & k=4\\ \left(1+x+x^3\right) & \to & k=4\\ (1+x)\left(1+x^2+x^3\right),x^i(1+x)\left(1+x^2+x^3\right)\ (i=1,2) & \to & k=3\\ (1+x)\left(1+x+x^3\right),x^i(1+x)\left(1+x+x^3\right)\ (i=1,2) & \to & k=3\\ \left(1+x^2+x^3\right)\left(1+x+x^3\right) & \to & k=1\\ (1+x)\left(1+x^2+x^3\right)\left(1+x+x^3\right) & \to & k=0 \end{array}$$

From this, we see that there are two such divisors which have $k=3$. This means that there are exactly two different binary $[7,3]$-cyclic codes.

For the first one, $(1+x)\left(1+x^2+x^3\right)=1+x+x^2+x^4$.

$$\begin{array}{lll} 0\cdot\left(1+x+x^2+x^4\right) & \to & 0000000\\ 1\cdot\left(1+x+x^2+x^4\right) & \to & 1110100\\ x\cdot\left(1+x+x^2+x^4\right) & \to & 0111010\\ x^2\cdot\left(1+x+x^2+x^4\right) & \to & 0011101 \end{array}$$

And the pairwisely exhaustive additions yield,

$$\begin{aligned} 1110100+0111010&=1001110\\ 1110100+0011101&=1101001\\ 0111010+0011101&=0100111\\ 1110100+0111010+0011101&=1010011 \end{aligned}$$

Therefore,

$$\left\langle(1+x)\left(1+x^2+x^3\right)\right\rangle=$$
$$\{0000000,1110100,0111010,0011101,1001110,0100111,1010011,1101001\}$$

#

Similarly for the second one,

$$\left\langle(1+x)\left(1+x+x^3\right)\right\rangle=$$
$$\{0000000,1011100,0101110,0010111,1001011,1100101,1110010,0111001\}$$

#